In the claims:

The claims in the application are indicated below:

1. (Currently amended) In a processing system including a server capable of communicating with ~~a client~~ plural clients via a ~~communications channel~~ computer network, a method of authenticating for a first client a data object that is provided by a second client, the method comprising the steps of, in the server,

~~(1)~~ receiving the data object transmitted from the second client to the server via the ~~communications channel~~ computer network;

~~(2)~~ generating at the server a signature corresponding to the second client by processing the data object;

~~(3)~~ associating the signature with the data object at the server to create a signed object; ~~and~~

delivering the signed object to the first client; and

~~(4) authenticating~~ returning the signed object from the first client to the server to authenticate that the signature of the signed object corresponds to the second client, ~~subsequently upon request, by: (a)~~ the authentication including deriving from the signed object information representative of the data object and the signature, ~~(b)~~ generating a comparison value using the information representative of the data object, and ~~(c)~~ determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

2. (Original) The method of claim 1 wherein the data object comprises a document.

3. (Currently amended) The method of claim 1 further including the ~~further~~ step of~~, in the server,~~ authenticating the second client at the server in connection with the second client transmitting the data object being to the server.

4. (Currently amended) The method of claim 3 wherein the second client is authenticated by the server using information representative of the client.

5. (Currently amended) The method of claim 4 wherein the information representative of the second client comprises a password provided ~~by~~ from the second client.

6. (Currently amended) The method of claim 3 wherein the second client is authenticated by the server using an encrypted data channel.

7. (Original) The method of claim 6 wherein the encrypted data channel utilizes a SSL protocol.

8. (Currently amended) The method of claim 3 wherein the second client is authenticated by the server using a public key-based processing step.

9. (Currently amended) The method of claim 8 wherein the public key-based processing step includes ~~the presentment~~ presentation of a client certificate.

10. (Currently amended) The method of claim 9 wherein the second client and server mutually authenticate using a zero-knowledge proof step.

11. (Currently amended) The method of claim 3 including the further step of~~, in the server,~~ creating and managing in the server a private ~~keys~~ associated with the second client, the private key being ~~to use~~ used in the step of generating the signature.

12. (Currently amended) The method of claim 11 wherein the server assigns ~~a~~ the private key to the second client.

13. (Currently amended) The method of claim 12 wherein the private key assigned to the second client is determined based upon ~~the~~ information representative of the second client.

14. (Currently amended) The method of ~~claim 13~~ claim 1 wherein the step of generating the signature includes the steps of~~:~~ assigning a private key to the second client; performing a predefined hash function on the data object to produce a hash total; and encyphering the hash total using the private key.

15. (Original) The method of claim 1 wherein the signed object comprises the signature and an address of the data object.

16. (Original) The system of claim 1 wherein the signed object comprises the signature and the data object.

17. (Currently amended) In a processing system comprising a server capable of communicating with ~~a client~~ plural clients via a ~~communications channel~~ computer network, a method of generating a digital signature, the method comprising the steps of~~, in the server~~:

receiving at the server a data object transmitted from ~~the~~ a signing client ~~to the server~~ via the ~~communications channel~~ computer network;

assigning a descriptor to the data object ~~a~~ at the server, the descriptor ~~containing~~ having a property field ~~, the property field containing~~ the includes a signature field;

~~assigning a private key, stored at the server, to the client;~~ processing the data object using a pre-determined hash function and ~~the~~ a private key to generate a signature, the private key being stored at the server in association with the client; ~~and~~

attaching the signature to the signature field ~~associated with~~ of the descriptor assigned to the data object to create a signed object; and

returning the signed object to the signing client for delivery to a receiving client.

18. (Currently amended) The method of claim 17 further including the ~~step~~ steps of~~, in the server,~~:

receiving the signed object at the server from the receiving client; and

authenticating the signed object at the server by verifying that the signature attached to the signature field of the signed object corresponds to the signing client.

19. (Currently amended) The method of claim 18 wherein ~~the verifying step~~ authenticating the signed object further comprises the steps of: ~~(a)~~ obtaining the data object from the signed object; ~~(b)~~ obtaining the signature from the signed object; ~~(c)~~ obtaining the private key stored at the server used to generate the signature; ~~(d)~~ processing the data object using a pre-determined hash function and the private key to generate a comparison value; and ~~(e)~~ determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

20. (Original) The method of claim 19 wherein the property field further comprises a timestamp.

21. (Currently amended) The method of ~~claim 20~~ claim 19 wherein the property field further comprises an identifier used to look up ~~a~~ the private key stored at the server.

22. (Original) The method of claim 19 wherein the property field further comprises key information used to generate the comparison value.

23. (Original) The method of claim 17 wherein the descriptor further comprises a plurality of property fields.

24. (Original) The method of claim 23 wherein at least one of the property fields further comprises data that is private to the server.

25. (Original) The method of claim 23 wherein at least one of the property fields further comprises additional data that is signed by a key private to the server.

26. (Original) The method of claim 25 wherein the additional data is derived by processing the data object using a pre-determined function.

27. (Original) The method of claim 26 wherein the pre-determined function is a hash function.

28. (Original) The method of claim 26 wherein the pre-determined function is a transform function.

29. (Original) The method of claim 25 wherein the additional data is obtained from a device.

30. (Original) The method of claim 29 wherein the device receives the data object prior to subsequent processing by the server.

31. (Original) The method of claim 29 wherein the device does not receive the data object.

32. (Original) The method of claim 29 wherein the device further comprises a device for generating a timestamp.

33. (Original) The method of claim 29 wherein the additional data, after being obtained from the device, is used by the server to generate the signature.

34. (Cancelled)

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Cancelled)

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled)

47. (Cancelled)

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (Cancelled)

53. (Cancelled)

54. (Cancelled)

55. (Cancelled)

56. (Currently amended) A digital signature server system ~~including:~~ on a server capable of communicating with ~~a client~~ plural clients via a ~~communications channel~~ computer network, ~~and means for authenticating a data object, further~~ comprising:

~~(1)~~ means for receiving ~~the~~ a data object transmitted from ~~the~~ a signing client to the server via the ~~communications channel~~ computer network;

~~(2)~~ means for generating at the server a signature corresponding to the signing client by processing the data object;

~~(3)~~ means for associating the signature with the data object to create a signed object; ~~and~~

means for receiving the signed object at the server from a client other than the signing client; and

~~(4)~~ means for authenticating that the signature of the signed object corresponds to the signing client, ~~subsequently upon request, by: (a)~~ including deriving from the signed object information representative of the data object and the signature, ~~(b)~~ generating a comparison value using the information representative of the data object, and ~~(c)~~ determining whether the comparison value and at least a portion of the signature meet a pre-determined criteria.

57. (Original) The system of claim 56 wherein the data object comprises a document.

58. (Currently amended) The system of claim 56 further comprising means for obtaining at the server information representative of the signing client to authenticate the signing client.

59. (Currently amended) The system of ~~claim 58~~ claim 56 further comprising means for creating and managing at the server a private ~~keys~~ key for the signing client used to generate the signature.

60. (Cancelled)

61. (Currently amended) The system of ~~claim 60~~ claim 59 wherein the private key is assigned to the signing client using ~~the~~ information representative of the client.

62. (Currently amended) The system of claim 56 wherein the means for generating a signature further ~~comprise:~~ comprises assigning a private key to the signing client; performing a predefined hash function on the data object to produce a hash total; and encyphering the hash total using the private key.

63. (Original) The system of claim 56 wherein the signed object comprises the signature and an address of the data object.

64. (Original) The system of claim 56 wherein the signed object comprises the signature and the data object.

65. (Currently amended) ~~A processing~~ In a digital signature server system ~~comprising:~~ having a server capable of communicating with ~~a client~~ plural clients via a ~~communications channel~~ computer network, ~~processing means in the server for generating a digital signature, further~~ a computer readable medium, comprising:

~~means~~ software for receiving a data object transmitted from ~~the~~ a signing client to the server via the ~~communications channel~~ computer network;

~~means~~ software for assigning to the data object a descriptor ~~containing~~ that includes a property field, ~~the property field containing~~ having a signature field;

~~means~~ software for assigning and storing at the server a private key, ~~stored at the server,~~ that corresponds to the signing client;

~~means~~ software for processing the data object using a pre-determined hash function and the private key to generate a signature; and ~~means for attaching~~ to attach the signature to the signature field associated with the data object to create a signed object; and

software to return the signed object to the signing client for delivery to a different client.

66. (Currently amended) The ~~processing system~~ medium of claim 65 further comprising:

software for receiving the signed object from the different client; and

~~means~~ software for authenticating the signed object.

67. (Currently amended) The ~~processing system~~ medium of claim 66 wherein the ~~means~~ software for authenticating the signed object ~~is further comprised of means for verifying~~ verifies that the signature attached to the signature field of the signed object corresponds to the signing client.

68. (Currently amended) The ~~processing system~~ medium of claim 67 wherein ~~the means for~~ verifying the signature further comprises: ~~(a) means for~~ obtaining the data object from the signed object; ~~(b) means for~~ obtaining the signature from the signed object; ~~(c) means for~~ obtaining the private key stored at the server used to generate the signature; ~~(d) means for~~ processing the data object using a predetermined hash function and the private key to generate a comparison value; and ~~(e) means for~~ determining whether the comparison value and at least a portion of the signature meet a predetermined criteria.

69. (Currently amended) The ~~processing system~~ medium of claim 67 wherein the property field further comprises a timestamp.

70. (Currently amended) The ~~processing system~~ medium of claim 67 wherein the property field further comprises an identifier used to look up a key stored at the server.

71. (Currently amended) The ~~processing system~~ medium of claim 67 wherein the property field further comprises key information used to generate the comparison value.

72. (Currently amended) The ~~processing system~~ medium of claim 67 wherein the descriptor further comprises a plurality of property fields.

73. (Currently amended) The ~~processing system~~ medium of claim 72 wherein at least one of the property fields further comprises data that is private to the server.

74. (Currently amended) The ~~processing system~~ medium of claim 72 wherein at least one of the property fields further comprises additional data that is signed by a key private to the server.

75. (Currently amended) The ~~processing system~~ medium of claim 74 wherein the additional data is derived by processing the data object using a pre-determined function.

76. (Currently amended) The ~~processing system~~ medium of claim 75 wherein the pre-determined function is a hash function.

77. (Currently amended) The ~~processing system~~ medium of claim 75 wherein the pre-determined function is a transform function.

78. (Currently amended) The ~~processing system~~ medium of claim 74 further comprising a device for providing the additional data.

79. (Currently amended) The ~~processing system~~ medium of claim 74 wherein the device receives the data object prior to subsequent processing by the server.

80. (Currently amended) The ~~processing system~~ medium of claim 74 wherein the device does not receive the data object.

81. (Currently amended) The ~~processing system~~ medium of claim 74 wherein the device further comprises a device for generating a timestamp.

82. (Currently amended) The ~~processing system~~ medium of ~~claim 74~~ claim 81 wherein the server generates the signature after obtaining ~~the~~ a timestamp from the device.

83. (Cancelled)

84. (Cancelled)

85. (Cancelled)

86. (Cancelled)

87. (Cancelled)

88. (Cancelled)

89. (Cancelled)

90. (Cancelled)

91. (Currently amended) The digital signature server system of ~~claim 90~~ claim 104 wherein the means for verifying the digital signature further comprises:

means for receiving the signed object from the verifying client;

means for obtaining the data object using information contained within the signed object;

means for obtaining the digital signature using information contained within the signed object;

means for obtaining the private key stored on the server using information contained within the signed object;

means for generating a comparison value using the data object; and

means for verifying the digital signature if the comparison value and at least a portion of the digital signature meet a predetermined criteria.

92. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the signed object comprises the digital signature and an address of the data object.

93. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the signed object comprises the digital signature and the data object.

94. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the signed object comprises the digital signature contained within the data object.

95. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the signed object comprises a hash of the data object contained within the digital signature.

96. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 further comprising means for authenticating a user before providing access to the system.

97. (Original) The digital signature system of claim 96 wherein means for authenticating a user further comprises means for receiving a user ID and a password from the client.

98. (Original) The digital signature system of claim 97 wherein the server assigns a private key to the client based upon the user ID.

99. (Original) The digital signature system of claim 98 wherein the server assigns a private key to the client based upon a system policy and data obtained from the client.

100. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the digital signature further comprises: a encrypted field; and a timestamp, wherein the server generates the encrypted field by hashing the data object according to a predefined hash function to create a hash, and encrypts the hash using the private key assigned to the user.

101. (Currently amended) The digital signature server system of ~~claim 91~~ claim 104 wherein the digital signature further comprises a server key.

102. (Original) The digital signature system of claim 100 further comprising: means for generating a verification response at the server; and means for transmitting the verification response to the client.

103. (Original) The digital signature system of claim 100 further comprising: means for generating a verification signature for the verification response at the server; and means for transmitting the verification signature to the client.

104. (New) A digital signature server system for use by plural remote clients in network communication with a server, the system comprising:

processing means on the server for generating a private key corresponding to a user at a signing client;

storing means on the server for storing the private key;

processing means for generating a digital signature using the private key for a data object provided by the user from the signing client, the processing means

performing a pre-defined hash function on the data object to create a hash value and performing a pre-defined encryption function using the private key on the hash value;

transmitting means for sending the digital signature from the server to the signing client within a signed object;

receiving means for receiving the signed object at the server from a verifying client that is different from the signing client; and

verifying means for verifying at the server that the digital signature in the signed object received from the verifying client corresponds to the user at the signing client.